FortiSwitch - Release Notes

3.6.2

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

August 30, 2017

FortiSwitch 3.6.2 Release Notes

11-362-445372-20170830

TABLE OF CONTENTS

Change log

Date	Change Description
2017-08-30	Initial release

Introduction

This document provides the following information for FortiSwitch 3.6.2 build: 0382.

See the Fortinet Document Library for FortiSwitch documentation.

Supported models

FortiSwitch 3.6.2 supports the following models:

FortiSwitch	FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-FPOE, FSW-224D-POE, FSW-248D-FPOE, FSW-248D-POE,FSW-248D, FSW-424D, FSW-424D-FPOE, FSW-424D-POE, FSW-448D, FSW-448D-FPOE, FSW-448D-POE, FSW-524D-FPOE, FSW-524D, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D
FortiSwitch Rugged	FSR-112D-POE, FSR-124D

What's new in 3.6.2

Release 3.6.2 provides the following new features:

- Spanning Tree Protocol (STP) root guard
- STP bridge protocol data unit (BPDU) guard
- Quality of service (QoS) queue counters
- IGMP snooping: static multicast groups
- SNMP: new port tagging status object identifier (OID)
- DHCP snooping: entry limit per port
- Network device detection
- Cycle redundancy check (CRC) verification of firmware images
- New REST API endpoints
- Improved error messages for failed REST API commands

NOTE: To use the `diagnose hardware sysinfo bootenv` command, you must have an advanced features license.

Special notices

Supported features for FortiSwitchOS 3.6

The following table lists the FortiSwitch features in Release 3.6 that are supported on each series of FortiSwitch models. All features are available in Release 3.6.0, unless otherwise stated.

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Link aggregation group size (maximum number of ports) (See Note 2.)	✓	8	8	24/48	24/48	24 (3.5.0) 64 (3.5.1)
Auto module max speed detection and notification	✓			✓	✓	
IP conflict detection and notification		✓	✓	✓	✓	✓
MAC-IP binding	✓			✓	✓	✓
Static BFD					✓	✓
Hardware-based ECMP	N/A			✓	✓	✓
Private VLANs	✓		✓	✓	✓	✓
LLDP transmit		✓	✓	✓	✓	✓
Loop guard	✓	✓	✓	✓	✓	✓
LAG min-max-bundle		✓	✓	✓	✓	✓
sFlow	✓	✓	✓	✓	✓	✓
Storm control	✓	✓	✓	✓	✓	✓
ACL			✓	✓	✓	✓
Static L3/hardware-based routing	✓		✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Software routing only	✓	✓				
CPLD software upgrade support for OS					✓	
PoE-pre-standard detection (See Note 1.)	✓	✓	✓	✓		
VLAN tag by ACL			✓	✓	✓	✓
ACL redirect to mirror destination as trunk/LAG			✓	✓	✓	✓
MAC/IP/protocol-based VLAN assignment	✓	✓	✓	✓	✓	✓
802.1x port mode	✓	✓	✓	✓	✓	✓
802.1x MAC-based security mode	✓		✓	✓	✓	✓
User-based (802.1x) VLAN assignment	✓	✓	✓	✓	✓	✓
Virtual wire	✓		✓	✓	✓	✓
HTTP REST APIs for configuration and monitoring	N/A	✓	✓	✓	✓	✓
Split port				✓		✓
IGMP Snooping			✓	✓	✓	✓
Per-port max for learned MACs			✓	✓		
802.1p support, including priority queuing trunk and WRED (release 3.5.1)			✓	✓	✓	✓
DHCP snooping			✓	✓	✓	✓
LLDP-MED		✓	✓	✓	✓	✓
DHCP relay feature			✓	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Support for switch SNMP OID		✓	✓	✓	✓	✓
802.1x enhancements, including MAB (release 3.5.1)	✓	✓	✓	✓	✓	✓
Multi-stage load balancing (release 3.5.1)					✓	✓
MCLAG (multichassis link aggregation)(release 3.6.0)		N/A	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic layer-3 protocols (OSPF, RIP, and VRRP) (release 3.6.0) (See Note 3.)	✓	N/A	✓ (not on 124D/124D-POE)	✓	✓	✓
Dynamic ARP inspection (release 3.6.0)		N/A	✓	✓	✓	✓
Firmware image rotation (dual-firmware image support) (release 3.6.0)		✓ (not on 108D-POE, 224D-POE)	✓	✓	✓	✓
TDR (time-domain reflec-tometer)/cable diagnostics sup-port (release 3.6.0)	✓	N/A	✓	✓	✓	✓
MAC learning limit (release 3.6.0) (See Note 4.)		N/A	✓	✓		
Sticky MAC on switch interfaces (release 3.6.0)		N/A	✓	✓	✓	✓
PoE modes support: first come, first served or priority based (PoE models) (release 3.6.0)		✓	✓	✓	N/A	✓
ACL: egress mask action sup-port (release 3.6.0)		N/A	✓ (not on 248Ds, 448Ds)	✓	✓	✓

Feature	GUI supported	108D-POE 112D-POE 224D-POE	124D 124D-POE 200 series 400 series	500 series	1024D 1048D	3032D
Monitor system temperature (threshold configuration and SNMP trap support) (release 3.6.0)		✓	✓	✓	✓	✓
'forced-untagged' or 'force-tagged' setting on switch interfaces (release 3.6.0)		✓	✓	✓	✓	✓
Selective packet sampling to CPU (useful diagnostic tool) (release 3.6.0)		N/A	✓	✓	✓	3.6.1
Add CLI to show the details of port statistics (release 3.6.0)		✓	✓	✓	✓	✓
Display progress (%) during firmware upgrade (release 3.6.0)	✓	✓	✓	✓	✓	✓
STP root guard (release 3.6.2)		✓	✓	✓	✓	✓
STP BPDU guard (release 3.6.2)		✓	✓	✓	✓	✓
QoS queue counters (release 3.6.2)				✓	✓	✓
IGMP snooping: static multicast groups (release 3.6.2)			✓	✓	✓	✓
DHCP snooping: entry limit per port (release 3.6.2)			✓	✓	✓	✓
Network device detection (release 3.6.2)			✓	✓	✓	✓

Notes

1. PoE features are applicable only to the model numbers with a POE or FPOE suffix.
2. 24-port LAG is applicable to 524D, 524_FPOE, 1024D, and 3032D models. 48-port LAG is applicable to 548D, 548_FPOE, and 1048D models.
3. To use the dynamic layer-3 protocols, you must have an advanced features license.
4. The per-VLAN learning limit is not supported on dual-chip platforms (248 and 448 series).

Default flow-control state changed to disable

This change allows a port to ignore the pause frame it receives. You can still enable flow control on a port if so desired by using the following CLI commands:

To enable flow control on *both* RX *and* TX:

```
S548DN4K16000360 # config switch physical-port
S548DN4K16000360 (physical-port) # edit port9
S548DN4K16000360 (port9) # set flow-control both
```

To enable flow control on RX only:

```
S548DN4K16000360 # config switch physical-port
S548DN4K16000360 (physical-port) # edit port9
S548DN4K16000360 (port9) # set flow-control rx
```

To enable flow control on TX only:

```
S548DN4K16000360 # config switch physical-port
S548DN4K16000360 (physical-port) # edit port9
S548DN4K16000360 (port9) # set flow-control tx
```

Connecting multiple FSW-R-112D-POE switches

The FSW-R-112D-POE switch does not support interconnectivity to other FSW-R-112D-POE switches using the PoE ports. Fortinet recommends using the SFP ports to interconnect switches.

Upgrade information

FortiSwitch 3.6.2 supports upgrading from FortiSwitch 3.5.0 and later.

Cooperative Security Fabric upgrade

FortiOS 5.4.1 greatly increases the interoperability between other Fortinet products. This includes:

- FortiClient 5.4.1
- FortiClient EMS 1.0.1
- FortiAP 5.4.1
- FortiSwitch 3.4.2

The upgrade of the firmware for each product must be completed in a precise order so the network connectivity is maintained without the need of manual steps. Customers must read the following two documents prior to upgrading any product in their network:

- *Cooperative Security Framework - Upgrade Guide*
- *FortiOS 5.4.0 to 5.4.1 Upgrade Guide for Managed FortiSwitch Devices*

  This document is available in the Customer Support Firmware Images download directory for FortiSwitch 3.4.2.

Product integration and support

FortiSwitch 3.6.2 support

The following table lists 3.6.2 product integration and support information.

Web browser	• Microsoft Internet Explorer version 11 • Mozilla Firefox version 52 • Google Chrome version 56 Other web browsers may function correctly, but are not supported by Fortinet.

FortiOS (FortiLink Support)	• 5.4.1 and later FortiSwitch must be upgraded first before upgrading FortiOS. Please read the *Upgrade Information* > *Cooperative Security Fabric Upgrade* section in this document. • 5.4.0 FortiSwitch models: FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSW-248D-POE, FSW-248D-FPOE, FSW-424D, FSW-424D-POE, FSW-424D-FPOE, FSW-448D, FSW-448D-POE, FSW-448D-FPOE, FSW-524D, FSW-524D-FPOE, FSW-548D, FSW-548D-FPOE, FSW-1024D, FSW-1048D, FSW-3032D, FSR-112D-POE FortiGate models: FG-60D, FG-60D-POE, FG-90D, FG-90-POE, FG-100D, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200D, FG-240D, FG-280D, FG-280D-POE, FG-600C, FG-800C, FG-1000C, FG-1500D, FG-1200D, FG-3700D, FG-3700DX FortiWiFi models: FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE • 5.2.3 and later FortiSwitch models: FSW-108D-POE, FSW-124D, FSW-124D-POE, FSW-224D-POE, FSW-224D-FPOE, FSR-112D-POE FortiGate models: FG-60D, FG-90D, FG-100D, FG-140D, FG-200D, FG-240D, FG-280D, FG-600C, FG-800C, FG-1000C, FG-60D-POE, FG-90D-POE, FG-140D-POE, FG-140D-POE-T1, FG-280D-POE FortiWiFi models: FWF-60D, FWF-60D-POE, FWF-90D, FWF-90D-POE • 5.2.2 FortiSwitch models: FSW-224D-POE FortiGate models: FG-90D, FG-90D-POE, FG-100D, FG-140D, FG-140D-POE, FG-140D-POE-T1, FG-200D, FG-240D, FG-280D, FG-280D-POE, FG-600C, FG-800C, FG-1000C FortiWiFi models: FWF-90D, FWF-90D-POE

Resolved issues

The following issues have been fixed in 3.6.2. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
444460	After a 424D OSPF router is started and builds the adjacency with neighbors successfully, it fails to keep the adjacency after about a day being up, causing OSPF functions to fail.
434688	When the ICL port is disabled on a MCLAG, the result is flooding on both peer FortiSwitches with bidirectional traffic.
443046	When two layer-3 FortiSwitches running OSPF or VRRP are interconnected through a layer-2 FortiSwitch in the same VLAN, the control packets are not forwarded.
443868	In a DHCP-snooping-enabled VLAN where the FortiSwitch has learned the IP addresses in the VLAN, the dhcp-snoop-learning-limit is being ignored.
443652	Multicast packets fail to forward to mRouter ports after a static group is configured.
416049	Using secure shell (SSH) to connect to the FortiSwitch using RADIUS authentication is not working.
442559	After a factory reset, the hardware configuration is not accepted.
443509	When a member interface of a static group receives an IGMP report and later an IGMP leave for the same group address, the interface stops receiving multicast packets until a reboot.
414455	IGMP control packets and layer-3 traffic is allowed through on an unauthorized dot1x port.
437229	After upgrading FortiSwitches from 3.5.0 to 3.5.5, there are a lot of STP log messages, and the eap_proxy daemon is being constantly restarted.
415240	When the TACACS+ authorization feature is enabled, the FortiSwitch is not getting authenticated.
438113	The LLDP advertisement packets are not changed when the global LLDP settings are changed.
393186	FortiSwitch does NOT allow time zones 00, 76, 82 and 86.
416704	Required IPv6 neighbor entries should remain more than 60 seconds.
406267	**Using the `execute restore secondary-image` command to place the image on the secondary partition, but the FortiSwitch booted from the primary partition.**

Known issues

The following known issues have been identified with 3.6.2. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
441840	When two FortiSwitches have the same IP address and are connected to the same VLAN on a management switch, no log message is generated.
423161	You cannot use the VLAN system interface to ping two neighboring FortiSwitches with IPv6 addresses.
440045	Configuring VLANs that have IGMP snooping enabled is slow. **Workaround:**Disable IGMP snooping on the trunk interface when configuring VLANs.
443999	When a port with BPDU guard enabled receives BPDUs and the port goes down, the GUI does not show that the port is down.
444484	A switched virtual interface that has DHCP mode enabled and DHCP snooping enabled cannot get the IP address from the DHCP server.
434680	Modifying or disabling a split port does not remove entries.
441901	EAP TLS authentication is not supported.
445355	The FortiSwitch does not route a packet when the destination MAC address was learned through a different interface.
393845	Newly created static MAC address may not get added in MAC address table when 802.1x feature is enabled on same interface.
410200, 393845	802.1x: VLAN programming received from a RADIUS server can be overwritten by CLI configuration. **Workaround:** Do NOT manually change the VLAN assignment on a port that is in an authentication state.
391607	Switch does not send gratuitous ARP for IP conflict when the system boots up and adds a new switch virtual interface (SVI).
414972	IGMP snooping may not work correctly when used with 802.1x Dynamic VLAN functionality.
416655	IGMP snooping may not work correctly when used with 802.1x Dynamic VLAN functionality.

Bug ID	Description
417024, 438441	DHCP client lease time on PVLAN is inaccurate.
417073, 438441	DHCP MAC address client is learned on Primary VLAN instead of the isolated VLAN.
417099, 438441	The system shows no DAI stats entry on PVLAN ports.
423161	The system is unable to ping two IPv6 neighbors using the VLAN system interface.
423940	In some cases, the MAC address and VLAN ID are shown (diagnostic command) twice on the same interface after splitting ports.
424096	(Access VLAN) A host in the same access VLAN can receive IGMP messages from other hosts.
434680	If you have a sticky-MAC address on an interface which is moved to split-port mode, some entries may remain. **Workaround:** Clear sticky-MAC address before changing to split-port mode.
380239	IGMP-snooped multicast groups are not immediately flushed out of the snooping table when the querier port is shut down.